

NDIA PRESENTATION

June 2000

Partners in Protection: The Future of Physical and Cyber Security



Thomas O'Hara
Sr. Field Security Adviser
World Bank





PART I: BANK ORGANIZATION AND MISSION



•
•
•

Bank Organization and Mission

- What we are not
- What we are
- Governors and Executive Directors

•
•
•

Bank Group Organization

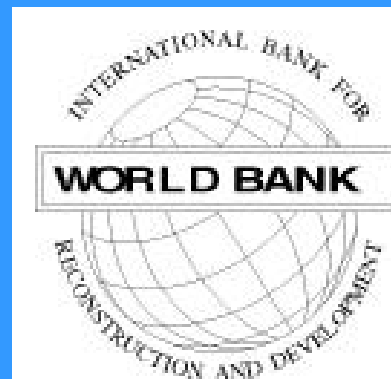
- IBRD – International Bank for Reconstruction and Development
- IDA – International Development Association
- IFC – International Finance Corporation
- MIGA – Multilateral Investment Guarantee Association
- ICSID – International Center for Settlement of Investment Disputes
- IBRD – Provides $\frac{3}{4}$ of annual lending

Bank Security Organizational Elements

- Fraud and Corruption – Legal and Anti-Corruption & Fraud (ACF)
- Crime and Internal Matters – Business Ethics & Integrity (BEI)
- Cyber – Information Systems Group (ISG)
- Physical Security and Executive Protection - Security

-
-
-
-
-
-
-
-
-
-

PART II: CYBER-SECURITY



-
-
-
-
-

•
•
•

Cyber Security

- Information System Group (ISG) -
Information Security Unit
- Information Security Program - Strategic Plan
 - Risk analysis
 - Policy
 - Standards
 - Mechanisms
 - Monitoring - auditing
and real-time
 - Trendy topics
- Point of contact: Frank O'Reilly(202) 473-4077

-
-
-
-
-
-
-
-
-
-

PART III: SECURITY



-
-
-
-
-

-
-
-

Security

Domestic – Physical, Fire Safety and Guard Force Management

Executive Protection – Team, Drivers

Field Security – Physical at 100+ Offices, Joint Secretariat Meetings

•
•
•

Historical Perspective

- More than 50 years without major problems
- Security focuses priority on Headquarters
- Field Security less emphasis
- Changing conditions change focus to Field Security

•
•
•

Risks to Bank

- Decentralization
- Anti-corruption focus
- World financial crisis
- Terrorism and increased crime
- No direct threats to Bank – isolated threats to staff

•
•
•

Risks to Field

- Terrorist Acts
- Package and letter bombs
- Mob violence
- Crimes of opportunity
- Armed assailants
- Corruption
- Workplace violence
- Family safety
- Fire/Life safety
- Kidnappings-Ransom

•
•
•

Travel/Threat Advisory

- Advisory available to staff via webpage
- Maintained daily
- Follows UN Five Phase System

•
•
•

Travel Briefings

- Available for all staff being assigned overseas
- Resident Representatives and Country Directors
- New Program – two page advisory

•
•
•

Crisis Management

- Natural – Earthquakes, floods, etc.
- Internal Conflict
- Kidnap and ransom
- Evacuations – Work with UN
- Security Operations Center (SOC)

•
•
•

Facility Design

- Security concerns for new office selection
- Office renovations and upgrades

•
•
•

Field Assessments

(Physical Security and Fire Safety)

- Residences
 - Security assessment
 - Family safety – local staff, guards
- Travel – business and travel

•
•
•

Offices

- Threat assessments
- Openness policy vs. access control
- Embassy and UN coordination – Field Security Officer
- Staff briefings
- Police/Fire officials
- Information security
- Hotels

Cyber and Physical Security Interface

- Laptop Protection - Procedures
- Business Continuity Program
- Annual Meetings – Prague



Point of Contact

World Bank Field Security

1818 H. Street N.W.

Washington D.C. 20433

(202) 458-4445

email: tohara@worldbank.org



NDIA PRESENTATION

June 2000

Partners in Protection: The Future of Physical and Cyber Security

Bank Organization and Mission

What we are not

What we are

Governors and Executive Directors

Bank Group Organization

IBRD – International Bank for Reconstruction and Development

IDA – International Development Association

IFC – International Finance Corporation

MIGA – Multilateral Investment Guarantee Association

ICSID – International Centre for Settlement of Investment Disputes

IBRD – Provides $\frac{3}{4}$ of annual lending

Bank Security Organizational Elements

Fraud and Corruption – Legal and Anti-Corruption & Fraud (ACF)

Crime and Internal Matters – Business Ethics & Integrity (BEI)

Cyber – Information Systems Group (ISG)

Physical Security and – Security

Executive Protection

Cyber Security

Information Systems Group (ISG) – Information Security Unit

Information Security Program – Strategic Plan

Risk Analysis

Policy

Standards

Mechanisms

Monitoring – Auditing and Real-time

Trendy Topics

Point of Contact – Frank O'Reilly (202) 473-6891

Security

Domestic – Physical, Fire Safety and Guard Force Management

Executive Protection – Team, Drivers

Field Security – Physical at 100+ Offices, Joint Secretariat Meetings

Field Security

Historical Perspective

- More than 50 years without major problems
- Security focuses priority on Headquarters
- Field Security less emphasis
- Changing conditions change focus to Field Security

Risks to Bank

- Decentralization
- Anti-corruption focus
- World financial crisis
- Terrorism and increased crime
- No direct threats to Bank – isolated threats to staff

Risks to Field

- Terrorist Acts
- Package and letter bombs
- Mob violence
- Crimes of opportunity
- Armed assailants
- Corruption
- Workplace violence
- Family safety
- Fire/Life safety
- Kidnappings-Ransom

Travel/Threat Advisory

- Advisory available to staff via webpage
- Maintained daily
- Follows UN Five Phase System

Travel Briefings

- Available for all staff being assigned overseas
- Resident Representatives and Country Directors
- New Program – two page advisory

Crisis Management

- Natural – Earthquakes, Floods, etc.
- Internal Conflict
- Kidnap and Ransom
- Evacuations – Work with UN
- Security Operations Center (SOC)

Facility Design

- Security concerns for new office selection

Office renovations and upgrades

Field Assessments (Physical Security and Fire Safety)

Residences

Security assessment

Family safety – local staff, guards

Travel – business and travel

Offices

Threat assessments

Openness policy vs. access control

Embassy and UN Coordination – Field Security Officer

Staff briefings

Police/Fire officials

Information Security

Hotels

Web Page - Intranet

Cyber and Physical Security Interface

Laptop Protection - Procedures

Business Continuity Program

Annual Meetings – Prague

Bank Organization

Before I tell you what the WB is, I want to tell you what it is not:

First - The WB is not a commercial bank, it is a development bank. This is an important distinction that is not always understood in some countries. Because some of the criminal element is not always composed of the best and brightest, we want to discourage the possible connection with a commercial bank. This was just the case last year when a group of 5 men dressed in black, wearing hoods and armed with automatic rifles and grenades entered an office of another international development bank demanding all their money. Prior to leaving empty handed and partially out of embarrassment, they demanded that no one ever disclose they were there. It is for this reason that we try to low-key the presence of the WB and encourage Bank officials to use signage at their facilities indicating IBRD. I will tell you shortly what that means.

Second - We are not the International Monetary Fund (IMF) nor are we associated directly with the Fund in its practices except for about two times a year when we join forces to co-sponsor the Spring and Annual Meetings. Because of the Fund's greater requirement for compliance, we sometimes become associated with them in the minds of others. For example, recently in Nigeria the Fund required the government to increase gas prices and because of the perceived relationship, some of our visiting missions personnel received death threats. The WB had nothing to do with the gas price increase.

What are we then? We are an international organization – a bank that loans money to developing countries.

WB is owned by more than 180 member countries whose views and interests are represented by a Board of Governors and a Washington-based Board of Directors. Of the approximate 10,000 Bank staff, the United States is only one member who is limited to about 18 percent of the staff.

The WB offers loans, advice, and an array of customized resources to more than 100 developing countries and countries in transition.

Governors – Member countries are shareholders who are the decision-makers. Each member nation appoints a governor and alternate governor to carry out these responsibilities.

Meetings – They meet annually at the Bank's Annual Meetings to decide policy. Because they meet only annually, every member government is represented at the Bank's Headquarters in Washington by an executive director. The five largest shareholders (US, United Kingdom, Germany, France, and Japan) each appoint an Executive Director while the other countries are represented by the remaining 19 Directors.

The Bank's focus is on eliminating poverty and is the largest provider of development assistance, committing about \$20 billion in new loans each year.

The Bank, which I refer to generally, is actually a Bank Group that consists of five closely associated institutions:

IBRD – International Bank for Reconstruction and Development

IDA – International Development Association

IFC – International Finance Corporation

MIGA – Multilateral Investment Guarantee Association

ICSID – International Centre for Settlement of Investment Disputes

IBRD – Accounts for about three-fourths of the Bank's annual lending. We recommend use of the IBRD title at our oversea facilities because the designation is recognized easily by our clients but not usually by the common criminal who may be looking for a bank to rob.

Cyber Security

Organization

Information Solutions Group (ISG)

Information Security Unit

Information Security Program – Strategic Plan

Objective – To identify, research and sponsor systems, policies and standards to ensure the security, integrity and reliability of Bank Group (Bank) information resources.

Plan Summary

Risk Analysis – Identifies what the Bank is trying to protect. It is achieved in a variety of ways, for example: a. Y2K – application owners in the Bank identified the criticality of all their systems. b. Penetration tests are conducted and consultants try to break into Bank systems.

Policy – This is the framework for the program defining high level rules, responsibilities and accountabilities.

Standards – Specific standards are prepared for various environments (operating systems and databases). Auditors use these to check for compliance. For example, there are 130 rules for Unix, something similar to NT, Oracle database, etc. System administrators are expected to implement these rules.

Mechanisms – Mechanisms have been and are currently being implemented to security the network. These include auditing software on the servers, firewall technology, Virtual Private Network (VPN) connections with some field offices (encrypting all communications), etc. (About ten ECA (Eur/Cent Asia) offices)

Monitoring – Two types:

a. Auditing: Software is run against every device on the network, including printers and desktops. From this we can see where there are any security weaknesses and forward an alert, along with the action to be taken, to appropriate resource owners. (Three scans a month are run.)

b. Real-time Monitoring: They review all activity in the DMZ (where our external web resides) and just inside the firewall. With our software, we constantly look for known hacking patterns – when one is detected, key staff are advised by the system in real-time (paging) and necessary remedial action is taken – have to be fast.

Trendy Topics –

Anti-virus Programs – They use an aggressive *anti-virus program*, checking on our Notes servers, at the mail gateway and on every desktop.

Attachments - They also *block certain attachments* that are considered risky at entry points to the mail system (to counter attacks such as the recent I LOVE YOU trojan).

Limit Protocols - They also *limit certain protocols* at routers and firewalls and limit ports which can be accessed from the outside.

Point of Contact – Frank O'Reilly (202) 473-6891